Técnico en Redes y Comunicaciones para Computadores

19

TODO SOBRE:

Windows NT

Novell 5.0

Intranet

Hardware de Redes

Proyecto Completo: Cableado Estructurado

En este fascículo:

Software

- Marcado Automático.
- Marcado Multilink.
- Seguridad de RAS.
- Servidores Centralizados y Distribuidos.
- Autentificación.
- Auditoria.

Hardware

- FDDI-II
- TPDDI
- Modelos de Propagación.
- Normativa de Interconexión.
- Naturaleza de las Ondas de Radio.

Argentina $3,30 - México N$ 27 - Chile $1.350 - Colombia $4.500 - Venezuela Bs. 1850
Perú S/.7,00 - Bolivia Bs.10 - Costa Rica ¢ 800 - Panamá B/2,50 - Guatemala

CODESIS
COMERCIALIZADORA EDITORIAL Y SISTEMAS LTDA.

Técnico en Redes y Comunicaciones para Computadores

Realizado y Editado por:

CODESIS
COMERCIALIZADORA EDITORIAL Y SISTEMAS LTDA.

Avenida 22 No. 40 - 77 Of. 302
Telefax: 337 7052 - 335 0481
244 5387 - 335 0767
368 7180 - 269 4037
Santafé dce Bogotá, D.C. - Colombia
E-mail:
codesis@multi.net.co
www.codesis.com.co

Esta es una obra editorial
Realizada y Editada por:
CODESIS LTDA.
Comercializadora Editorial
y Sistemas Ltda.

Presidente: Jesús Rueda S.
Gerente General: Gustavo Rueda S.
Subgerente General: Germán Salazar D.
Autores:
Hardware/Software/Comunicaciones:
Gustavo Rueda S.
Jesús Rueda S.
Dirección Técnica y Proyectos
Gustavo Rueda S.
Diseño y Programación:
Yamile Assis R.
Miguel I. Morales V.
Juan D. García (CD-Roms)
Junta Administrativa:
Gloria Rueda S.
Norberto Cárdenas R.

© CODESIS LTDA., 2.000
Santafé de Bogotá - Colombia

Todos los derechos reservados, prohibida su reproducción total o parcial por cualquier medio sin permiso escrito del editor.

ISBN: 958-96430-3-5

Impreso en Colombia.
Printed In Colombia
Impreso por Printer Colombiana S.A.

La obra **TECNICO EN REDES Y COMUNICACIONES PARA COMPUTADOR** de **CODESIS LTDA., Comercializadora Editorial y Sistemas Ltda.** Es una publicación de aparición semanal en forma de 40 (cuarenta) fascículos, encuadernables en 4 (cuatro) volúmenes.
Cada fascículo consta de 4 páginas cubiertas y 20 páginas de contenido a todo color, que se dividen en Software y Hardware.
Las páginas de cada sección son encuadernables por separado, por esta razón al formar los volúmenes, debe cuidarse de desprender previamente, de todos los fascículos, las páginas de cada uno de los temas (Software y Hardware).
Durante la publicación de los fascículos, se pondrán a la venta las tapas de los 4 volúmenes de la obra para su respectiva encuadernación.
En la contraportada interior (tercera de portada) de cada fascículo, encontrará un test de **20** preguntas de evaluación de los temas tratados en él, para establecer los logros obtenidos y el nivel de aprendizaje alcanzado. Si desea obtener el título que lo acredita como **TECNICO EN REDES Y COMUNICACIONES PARA COMPUTADOR**, deberá enviarlos debidamente resueltos los 40 test (se pueden enviar uno a uno ó todos los 40 al final de la obra) a nuestra dirección en Santafé de Bogotá o nuestro e-mail: codesis@multi.net.co; luego de la respectiva calificación y aprobación podrá obtener el **DIPLOMA**.

CODESIS LTDA., Garantiza la total publicación de la obra, el suministro de las tapas necesarias para su encuadernación y el servicio de números atrasados hasta después de un año de terminada la circulación del último fascículo. Garantiza también la calidad del presente material, así como la entrega de los CD-Rom durante el desarrollo de la obra. Sin embargo no se responsabiliza por posibles daños en equipos, hardware, software o información causados por la manipulación errónea de éstos o por defectos en su fabricación o utilización.

CODESIS LTDA., No asume ninguna responsabilidad por daños y/o perjuicios que pudieran resultar de la información contenida en esta obra.
La utilización de cualquier término en esta colección no debe interpretarse como usurpación ilegal de ninguna marca registrada.

MARCAS REGISTRADAS:
COMPAQ (Compaq Computer Corporation) - IBM (international Busines Machines) - MS-DOS/Windows 3.1/Windows 95/Windows 98/Windows NT Server/Windows NT Workstation/Lan Manager (Microsoft Corporation) - Netware y Novell (Novell) - 3Com/Cardfacts/Etherlink/Linkbuilder/Parallel Tasking/Netbuilder/Lanplex/Acces Builder/SmartAgent/Superstack/FDDILink/ATMLink/Autolint (3Com Corporation) - Netscape Navigator (Netscape Comunication Corporation) - Apple y Macintosh (Apple Computer Inc.) -0 HP y Laserjet (Hewlett Packard) - Epson (Epson Corporation) - SMC (Standar Macrosystem Corporation)

DISTRIBUCION INTERNACIONAL:

Colombia:	DISTRIBUIDORAS UNIDAS S.A.	Teléfono:413 9300 (Santafé de Bogotá)
México:	DISTRIBUIDORA INTERMEX S.A.	Teléfono:230 9500 (México D.F.)
Venezuela:	DISTRIBUIDORA CONTINENTAL	Teléfono:4064 111 (Caracas)
Argentina:	DISTRIBUIDORA BERTRAN (Interior)	Teléfono:43031870(Buenos Aires)
	DIST. VACCARO SÁNCHEZ (Capital)	Teléfono:43031871(Buenos Aires)
Chile:	DISTRIBUIDORA ALFA S.A.	Teléfono:5255599 (Santiago)
Ecuador:	DISTRIBUIDORA DE LOS ANDES S.A.	Teléfono:271 644 (Guayaquil)
Perú:	DISTRIBUIDORA BOLIVARIANA S.A.	Teléfonos: 441 3160 (Lima)
Panamá:	DISTRIBUIDORA PANAMEX S.A.	Teléfono: 221 7015 (Panamá)

REALIZADO Y EDITADO POR:

CODESIS
COMERCIALIZADORA EDITORIAL Y SISTEMAS LTDA.

Avenida 22 No. 40 - 77 Of. 302
Teléfonos: 337 7052 - 335 0481 - 244 5387
Santafé de Bogotá, D.C. - Colombia
E-mail: codesis@multi.net.co

Solución de problemas de marcado automático

Si tiene problemas, ejecute el siguiente comando desde la interface de comandos para obtener información básica sobre el estado de **Marcado automático**:

C:> rasautou -s

La salida de la información de estado tiene dos partes: enlaces a la tarjeta adaptadora de red y una lista de las direcciones de Marcado automático aprendidas.

Al menos debe informar de que hay un enlace de una tarjeta adaptadora de red que funciona con **Marcado automático** para darse cuenta de que está conectado a la red.

Para que **Marcado automático** cree una nueva conexión de red, cuando ya está conectado a ella, la dirección debe estar en la lista de direcciones aprendidas de **Marcado automático**. He aquí un ejemplo de los enlaces de las tarjetas adaptadoras de red y una lista de las direcciones aprendidas: Comprobando enlaces de tarjeta de red... Red conectada: la red (\Device\Nbf_IEEPRO1, 0) está funcionando enumerando direcciones de **Marcado automático**...

Hay 3 direcciones de **Marcado automático**:

- ftp.microsoft.com
- 198.105.232.1
- SCRATCH

Marcado Multilink

Multilink combina varios vínculos físicos en un "manojo" lógico. Este vínculo agregado incrementa el ancho de banda. **RAS** realiza marcado **Multilink** punto a punto sobre varias líneas **ISDN (RDSI)**, X.25 o de módem. Esta característica sólo está disponible si el equipo tiene múltiples adaptadores de WAN. Para poder usar **Multilink**, debe estar activado en los clientes y en los servidores.

Una situación que funcionará es si la entrada de la guía telefónica multivínculo es **RDSI (ISDN)** con dos canales que tienen el mismo número de teléfono.

Para activar **Multilink** en un cliente **RAS** siga los siguientes pasos:

1) En **Conexión telefónica a la red**, seleccione una entrada para marcar de la guía telefónica.

2) Haga click en **Más** y seleccione **Editar entrada y propiedades del módem**.

3) En la ficha **Básico**, en el cuadro **Marcar utilizando**, seleccione **Líneas múltiples**.

4) Haga click en **Configurar para elegir los modems** o adaptadores que va a usar para la conexión y, a continuación, haga click en **Aceptar**. Para activar **Multilink** en un servidor **RAS** siga los siguientes pasos:

1) En el **Panel de control**, haga click en el ícono **Red**.

2) En la ficha **Servicios**, seleccione **Servicio de acceso remoto** en el cuadro **Servicios de red** y haga click en **Propiedades**.

NOTA

Si un cliente usa una entrada de la guía telefónica multivínculo para marcar un servidor que está configurado para devolver la llamada al usuario por razones de seguridad (devolución de llamada forzada), solamente se devolverá la llamada a uno de los dispositivos multivínculo. La razón de este funcionamiento se debe a que solamente se puede almacenar un número en la cuenta de usuario. Por tanto, solamente un dispositivo se conectará y todos los demás no podrán completar la conexión, y el cliente perderá la funcionalidad multivínculo.

3) En el cuadro de diálogo **Instalación de acceso remoto**, haga clik en **Red.**

4) En el cuadro de diálogo **Configuración de red**, seleccione la casilla de verificación **Activar enlace múltiple** y haga click en **Aceptar**.

Monitorización de conexiones

Monitor de Acceso telefónico a redes (ubicado en el **Panel de control**) proporciona el estado de una llamada y le permite ver:

- La velocidad de conexión.
- La duración de la conexión.
- Los nombres de los usuarios conectados a un servidor **RAS**.
- Los protocolos usados durante la conexión.
- Los dispositivos que forman parte de la conexión.

Seguridad de RAS

Las cuentas de usuario y los dominios de **Windows NT** proporcionan seguridad mediante autentificación cifrada. **RAS** proporciona características de seguridad adicionales como devolución de llamada y codificación de datos. También puede instalar hosts de seguridad de terceros para evitar accesos sin autorización a su **LAN**. Este capítulo describe las siguientes características de seguridad de **RAS**:

- Configuración de **RAS** en un dominio.
- Asignación de permiso **RAS** a cuentas de usuario.
- Configuración de la seguridad de **RAS** en cuentas de usuario.
- Codificación de datos.
- Seguridad con devolución de llamada.
- Soporte de hosts de seguridad.
- Auditoría.

Configuración de RAS en un dominio

La aplicación de la seguridad de **RAS** en los clientes se compone de tres pasos: la configuración de **RAS** en un dominio de **Windows NT**, la asignación de permiso **RAS** a cuentas de usuario de **Windows NT** y la configuración de la seguridad de **RAS** en dichas cuentas.

En esta sección se explican las cuentas de usuario de **Windows NT** y las técnicas de implementación de la seguridad de **RAS** en un dominio. Esta sección asume que tiene establecida una estructura de dominios y proporciona información acerca de la integración de **RAS** en la estructura de dominios existente.

Los servidores de Acceso remoto que utilicen la seguridad de dominio de **Windows NT Server** se pueden centralizar en un único dominio o distribuirse entre varios dominios que podrían tener relaciones de confianza.

Servidores centralizados

Si su objetivo es simplificar la administración, centralice todos los **servidores de Acceso remoto** en un único dominio: sólo tendrá que mantener una base de datos de cuentas de usuario y el

CODESIS COMERCIALIZADORA EDITORIAL Y SISTEMAS LTDA.

NOTA

Como el dominio es un concepto lógico más que físico, los servidores centralizados pueden encontrarse en ubicaciones diferentes y seguir formando parte del mismo dominio.

administrador del sistema podrá monitorizar todos los servidores y usuarios de **RAS** al mismo tiempo. (Use relaciones de confianza si cada departamento mantiene su propias cuentas de usuario).

En el modelo de dominios de confianza, lo mejor es definir una cuenta de usuario por cada usuario en sólo un dominio, especialmente para los usuarios que se conecten mediante **RAS versión 1.1** o anterior. Si el servidor de **Acceso remoto** no puede encontrar la cuenta del usuario en el dominio del servidor, comprueba simultáneamente los dominios de confianza y acepta la primera respuesta.

Si la primera respuesta viene de un dominio en el que el usuario tiene una contraseña diferente o no tiene permiso de **Acceso remoto**, la autentificación falla incluso aunque una segunda respuesta desde otro dominio pudiera indicar que la cuenta de usuario tiene permiso de **Acceso remoto.**

Servidores distribuidos

Las organizaciones más pequeñas que dan valor a la flexibilidad y al control local, o las organizaciones que no tienen una necesidad clara de seguridad centralizada, podrían preferir un sistema de servidores distribuidos, en el que cada departamento o grupo de trabajo configura y mantiene sus propios dominios de **Acceso remoto**.

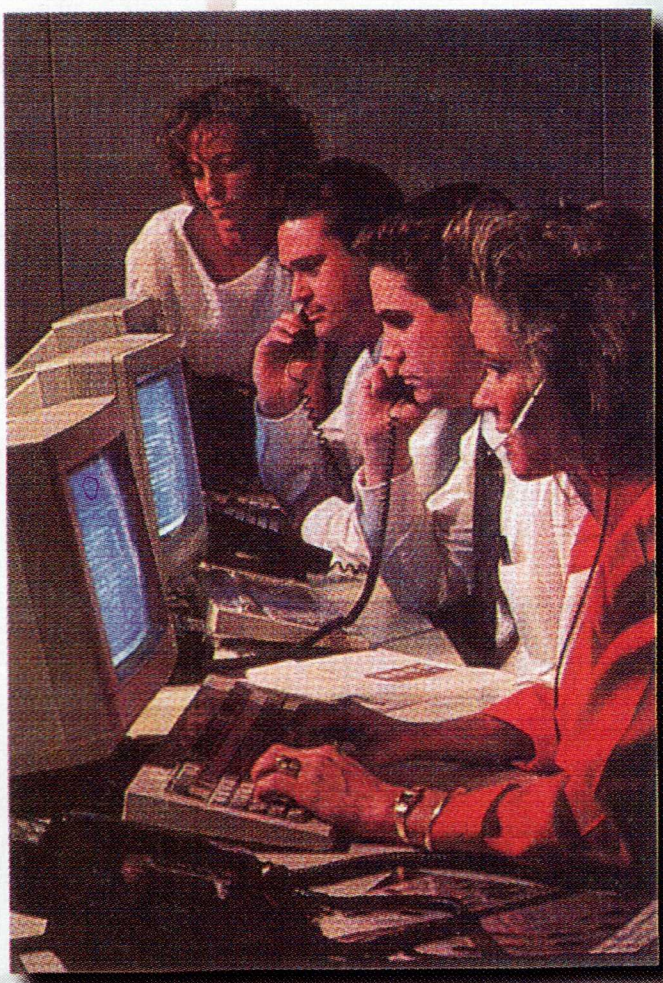
Para permitir el acceso entre los dominios se pueden utilizar relaciones de confianza.

Asignación de acceso y permisos RAS

Después de instalar un servidor **RAS**, tiene que especificar quién puede conectar con él. Para seleccionar cuentas de usuario de un equipo o de un dominio, use el programa **Administrador de acceso remoto.**

Después asigne permiso de **RAS** a las cuentas de usuario, como se muestra en las secciones siguientes. Después de pasar la autentificación de **Acceso remoto** y conectar con la **LAN**, los usuarios remotos pueden tener acceso a los recursos del servidor de aplicaciones para los que tengan permiso.

No tiene que crear cuentas de usuario sólo para los usuarios de **RAS**. Los servidores **RAS** usan las cuentas de usuario de cualquier dominio de confianza o equipo de la red **Windows NT.**



Para obtener información acerca de la inclusión de clientes remotos en un dominio.

NOTA

En los últimos años la digitalización de las redes telefónicas públicas conmutadas (PSTN), ha ido preparando al mundo, gracias al diseño modular. Varias ventajas de la digitalización de la red pueden ser la reducción de los gastos de explotación, de mantenimiento y de existencia de repuestos, hasta el propio nivel de instalación del cliente.

RECUERDE

Los privilegios de acceso remoto se asignan o deniegan de usuario en usuario. Por tanto, aunque RAS se ejecute en un equipo con Windows NT Server, el acceso a la red debe permitirse de forma explícita para cada usuario que lo necesite.

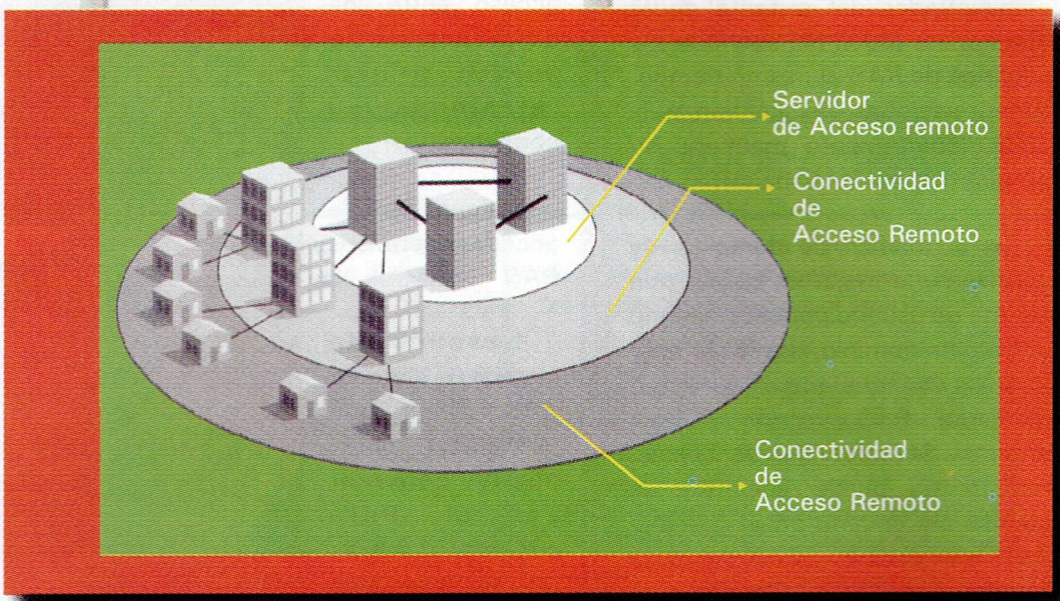
Configuración de la seguridad de RAS en las cuentas

Los usuarios remotos tienen que estar autentificados por un **servidor de Acceso remoto** antes de poder tener acceso o generar tráfico en la red. Esta autentificación es un paso diferente del inicio de sesión en **Windows NT**.

Las contraseñas de los usuarios y el procedimiento de autentificación se codifican cuando se transmiten a través de las líneas telefónicas.

Puede restringir el acceso a la red y al servidor de **Acceso remoto** por parte de los usuario remotos. Esto permite que un administrador controle con precisión la información disponible para los usuarios remotos, además de limitar su disponibilidad en caso de una ruptura de la seguridad.

Para obtener más información acerca de la asignación del permiso **RAS** a los usuarios, vea la Ayuda en pantalla del **Administrador de acceso remoto**.



NOTA

Los usuarios remotos están sujetos a la seguridad de Windows NT Server, como si estuviera en la oficina. Es decir, no pueden hacer nada para lo que no tengan el privilegio necesario, ni pueden tener acceso a los recursos para los que no tengan permiso.

Restricción de usuarios remotos en el servidor de acceso remoto

Incluso si el **servidor de Acceso remoto** está conectado a una red, puede restringir a los usuarios remotos el acceso al servidor al que llaman.

Funcionamiento de la seguridad en la conexión

Los siguientes pasos muestran lo que ocurre durante una llamada desde un cliente a un servidor **RAS**:

1) Mediante **Acceso telefónico a redes**, un cliente llama a un servidor de **Acceso remoto**.

2) El servidor envía una pregunta al cliente.

3) El cliente envía una respuesta codificada al servidor.

4) El servidor comprueba la respuesta en la base de datos de usuarios.

5) Si la cuenta es válida, el servidor comprueba que tiene permiso de **Acceso remoto**.

6) Si tiene asignado el permiso de **Acceso remoto**, el servidor conecta al cliente.

Si la devolución de llamada está habilitada, el servidor vuelve a llamar al cliente y repite los pasos 2 al 6.

Características de seguridad

Las características de la seguridad de **RAS** incluyen la codificación de las contraseña utilizando diferentes formas de protocolos de autentificación, la codificación de datos para mantener la seguridad en el caso de la interceptación no autorizada de las transmisiones de acceso remoto y la seguridad de devolución de

CODESIS COMERCIALIZADORA EDITORIAL Y SISTEMAS LTDA.

NOTA

Cuando se usa RAS en un entorno de dominio, los cambios de permiso de Acceso remoto no tienen efecto de manera inmediata en todos los servidores. Puede que la duplicación del cambio en los demás servidores del dominio tarde hasta 15 minutos. Si es necesario, puede volver a sincronizar el dominio para asegurarse de que un usuario con permisos denegados no pueda tener acceso a la red antes de que el cambio quede duplicado de la forma automática.

llamadas para predeterminar un número de cliente antes de permitir el acceso a la red.

Autentificación

La autentificación es un aspecto importante en muchas organizaciones. Esta sección muestra cómo **RAS** contribuye a asegurar la privacidad de las contraseñas.

Protocolos de autentificación

RAS usa el **Protocolo de autentificación de reto** (**CHAP**) para negociar la forma más segura de autentificación codificada aceptada tanto por el servidor como por el cliente. **CHAP** utiliza un mecanismo de pregunta-respuesta con una codificación unidireccional en la repuesta. **CHAP** permite que el servidor **RAS** negocie el mecanismo de codificación desde el más seguro al menos seguro y protege las contraseñas transmitidas en el proceso.

CHAP permite el uso de varios tipos de algoritmos de codificación. Específicamente, **RAS** utiliza **DES** y **MD5** de **RSA Security Inc. Microsoft RAS** utiliza la codificación **DES** cuando el cliente y el servidor utilizan **RAS**.

La codificación **DES** (estándar del gobierno de EE.UU.) se diseñó para proteger el descubrimiento y reproducción de las contraseñas. **Windows NT 3.5** o posterior, **Windows para Trabajo en Grupo** y **Windows95** siempre negocian la autentificación con codificación **DES** cuando se comunican entre sí.

Cuando se conectan con servidores de acceso remoto o software de cliente de terceros **RAS** puede negociar la autentificación mediante **SPAP** o texto normal si el producto no acepta la autentificación codificada. El cliente **RAS** de **Microsoft** puede negociar **MD5**, un esquema de codificación utilizado por varios fabricantes de **PPP** en la autentificación codificada, al conectar con servidores de acceso remoto de otros fabricantes. **MD5** no se encuentra disponible en el servidor **RAS**.

El Protocolo de autentificación de contraseñas de **Shiva** (**SPAP**) es un mecanismo de codificación bidireccional (reversible) empleado por **Shiva**. **Windows NT Workstation**, cuando se conecta con un **Shiva LAN Rover**, utiliza **SPAP**, al igual que un cliente **Shiva** cuando se conecta con un equipo con **Windows NT Server**.

Este modo de autentificación es más seguro que el texto normal pero menos que **CHAP**.

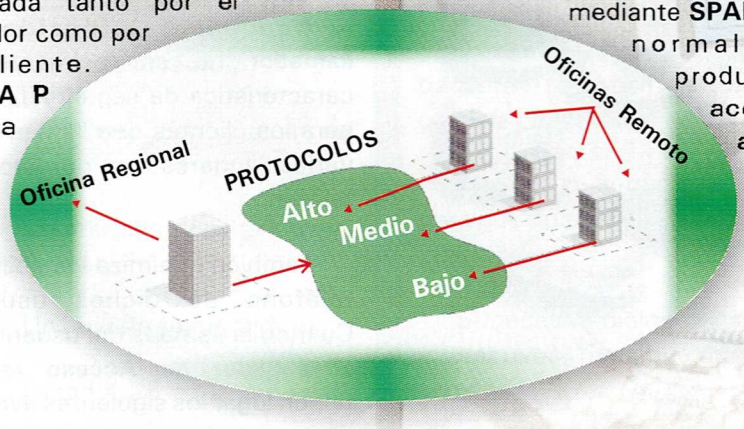
El Protocolo de autentificación de contraseña (**PAP**) utiliza contraseñas en texto normal y es el protocolo de autentificación menos sofisticado. Se negocia normalmente si la estación de trabajo remota y el servidor no pueden negociar una forma de validación más segura.

El servidor **RAS de Microsoft** tiene una opción que evita la negociación de contraseñas en texto normal.

Esta opción permite que los administradores de sistemas establezcan un nivel de seguridad mayor.

Niveles de seguridad y protocolos de codificación de RAS

Nivel de seguridad de codificación	Protocolo de codificación de RAS
Alto	Unidireccional CHAP, Md5
Medio	Bidireccional SPAP
Bajo	Texto normal PAP



Codificación de datos

La codificación de datos protege los datos y asegura las comunicaciones telefónicas. Esto es especialmente importante para instituciones financieras, agencias legales y gubernamentales, y para empresas que requieran transmisiones de datos seguras.

En instalaciones en las que se requiera seguridad total, el administrador de **RAS** puede configurar el servidor **RAS** para forzar que las comunicaciones estén codificadas. Los usuarios que se conecten con dicho servidor codifican automáticamente todos los datos enviados.

RAS proporciona codificación de datos además de la codificación de contraseñas como se describe en la sección "**Autentificación**".

Para mantener la seguridad en el caso de interceptaciones no autorizadas de las transmisiones de acceso remoto, los clientes configuran sus entradas de la guía telefónica para que usen codificación de datos. **RAS de Windows NT** proporciona codificación de datos utilizando el algoritmo **RC4** de **RSA™ Data Security Incorporated.**

Devolución de llamada

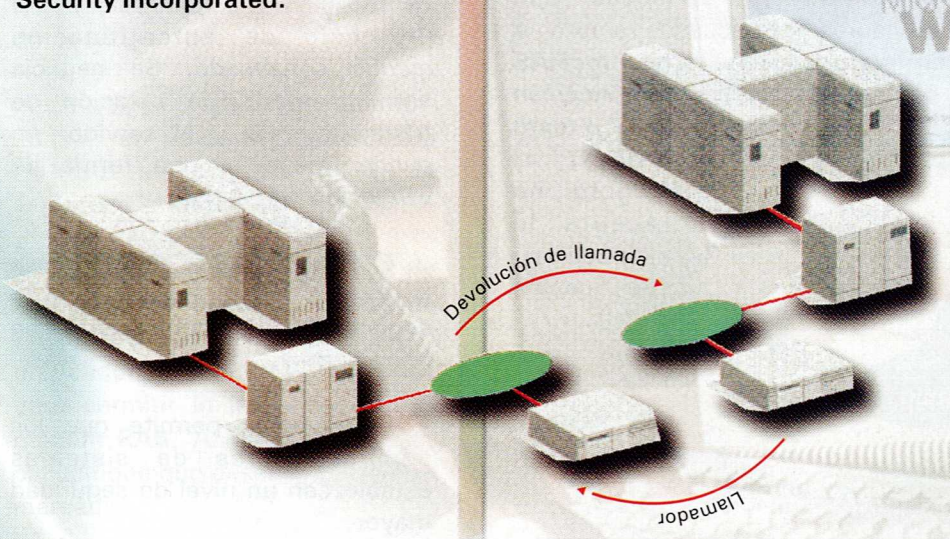
Como medida de seguridad adicional, **RAS** ofrece la característica **Devolución de llamada**, que asegura que sólo los usuarios de ubicaciones específicas puedan tener acceso al servidor **RAS**. También ahorra los gastos de teléfono al usuario.

Cuando se usa la **devolución de llamada**, el usuario inicia una llamada y conecta con el servidor **RAS**.

A continuación, el servidor **RAS** termina la llamada y llama inmediatamente al número de devolución de llamada previamente asignado. Este método de seguridad frustra las intenciones de la mayoría de los intrusos.

En el Administrador de acceso remoto, el cuadro de diálogo Permisos de acceso remoto contiene las opciones de devolución de llamada que puede elegir:

- Preestablecido a
- Establecido por llamador
- No devolver llamada (predeterminado)



NOTA

Hasta que no se haya autentificado y devuelto la llamada (si se ha configurado así) al usuario, no se transfieren datos desde el cliente ni desde el servidor de Acceso remoto.

Para obtener la mayor seguridad, seleccione **Preestablecido a** y escriba el número de teléfono al que está conectado el módem del usuario.

Cuando la llamada del usuario llega al servidor de Acceso remoto, el servidor ejecuta los siguientes pasos:

1). Determina si el nombre y la contraseña del usuario son correctos.

2) Si lo son, responde con un mensaje que anuncia que se va a devolver la llamada al usuario.

3) Desconecta y devuelve la llamada al usuario en el número predefinido.

Establezca esta opción para los equipos remotos estacionarios, como los de oficinas domésticas.

Establecido por llamador

Aunque **Establecido por llamador** no es realmente una característica de seguridad, es útil para los clientes que llamen desde varios lugares y números de teléfono.

También minimiza los gastos de teléfono de dichos usuarios. Cuando la llamada del usuario llega al **servidor de Acceso remoto**, tienen lugar los siguientes eventos:

CODESIS COMERCIALIZADORA EDITORIAL Y SISTEMAS LTDA.

La clase de servicio síncrono responde a aplicaciones que necesitan una banda de paso de alta capacidad y/o un tiempo de propagación en el encaminamiento determinado, con problemas si varían estos tiempos. La clase de servicio asíncrono satisface los inconvenientes de tráfico de tipo asíncrono, presentando cierta cantidad de banda de paso compartida por todas las estaciones que utilicen este método.

Con el fin de ofrecer un servicio satisfactorio al tráfico síncrono, el tiempo de rotación del testigo está controlado. Es decir, que el tiempo total utilizado por el testigo para recorrer toda la red debe resultar inferior a un umbral determinado por las aplicaciones que utilicen la red.

Un valor determina el tiempo de rotación del testigo: el TTRT (Target Token Rotation Time), que se establece durante la inicialización de la red. El valor TTRT se carga en un temporizador, llamado TRT (Token Rotation Timer) que controla la adquisición del testigo para la transmisión de las tramas en espera.

El testigo puede ser capturado para transmitir una trama síncrona independientemente del valor del TRT, mientras que sólo será código para transmitir una trama asíncrona si el tiempo del TRT no ha expirado. Opcionalmente, pueden distinguirse varios niveles de prioridad dentro del tráfico asíncrono de una estación, lo que permite controlar la banda de paso ofrecida a estas diferentes fuentes asíncronas.

Cuanto más elevada sea la prioridad de una estación, mayor es la banda de paso disponible para las fuentes asíncronas de esa prioridad.

c) El subnivel SMT

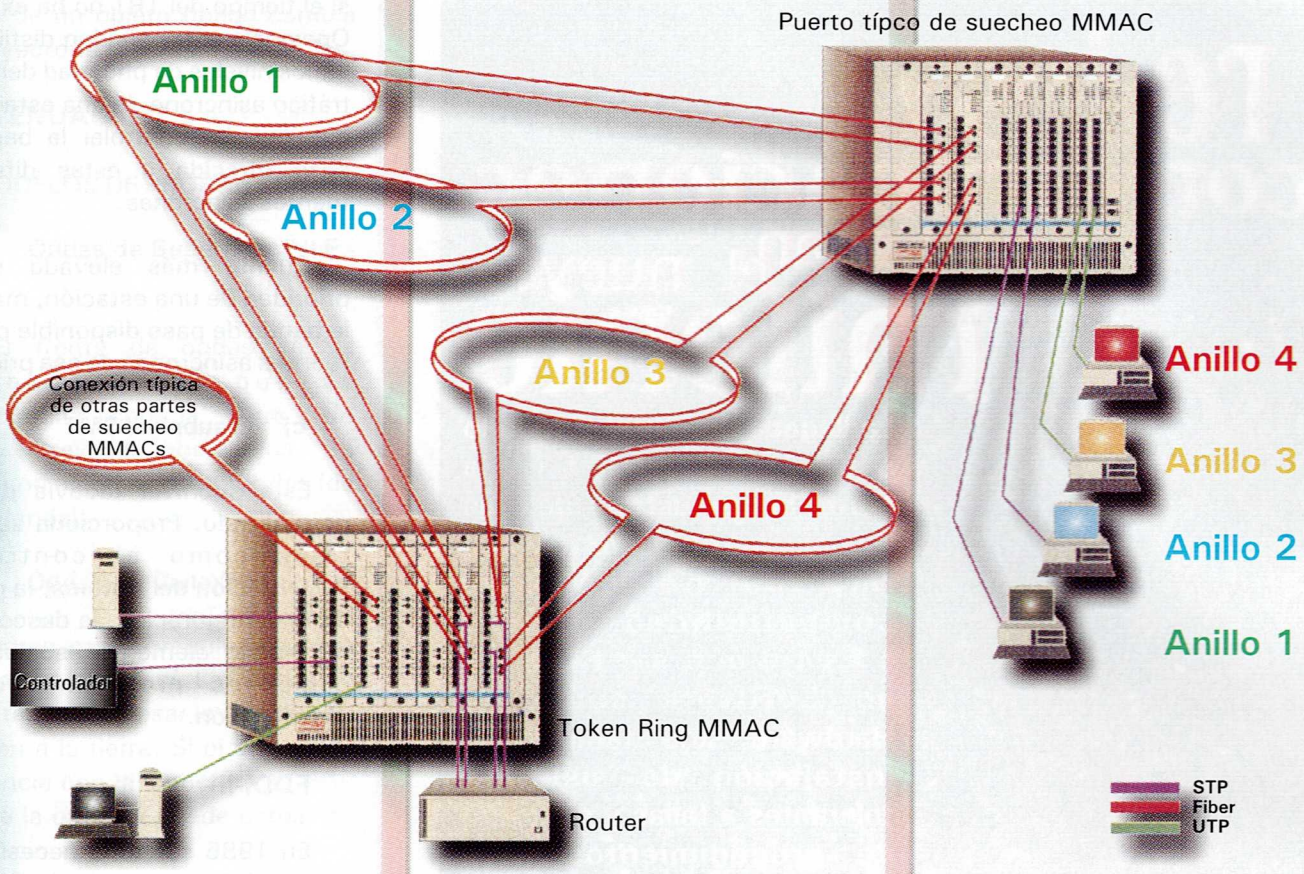
Este subnivel todavía no está normalizado. Proporciona servicios tales como el control de inicialización del sistema, la gestión de la configuración, la desconexión del nuevo elemento asociado, así como los procedimientos de planificación.

FDDI-II

En 1985 surgió la necesidad de una red local capaz de soportar simultáneamente voz y datos. El protocolo FDDI-I se reveló inadecuado para este tipo de aplicación, principalmente en redes con gran número de nodos.

Así, pues, se propuso una nueva versión del bucle FDDI, principalmente a iniciativa de especialistas en telecomunicaciones, como la British Telecom y AT&T, también basada sobre bucles de fibra óptica.

A fin de ofrecer una calidad de servicio adecuada para la voz, el protocolo FDDI-II utiliza una técnica de conmutación híbrida. De esta forma, la norma FDDI-II ofrece procedimientos de conmutación de circuitos para tráficos de voz y vídeo y, de conmutación de paquetes, para los datos. FDDI-II es una propuesta de norma americana de la ANSI (Comité X3T9.5) para



Conectividad multicanal Token Ring

una red local de 100 Mbits/s de capacidad con una longitud de más de 50 km. Se trata de un doble bucle, con control de acceso por testigo. FDDI-II es una extensión de la norma FDDI-I, que añade una trama síncrona.

La banda de paso está constituida por la trama asíncrona y 16 canales síncronos que contienen 96 "cyclic groups" de 16 bytes cada uno. El flujo síncrono alcanza, por consiguiente, 16x96x8/125 ?s = 98.304 Mbits.

TPDDI o CDDI

La norma FDDI ha sido ideada hace más de diez años para ser utilizada exclusivamente con fibra óptica; sin embargo, sus principios pueden aplicarse a pares trenzados.

La utilización de la FDDI sobre pares trenzados: TPDDI (Twisted PAir Distributed Data Interface), llamada incluso CDDI (Copper Distributed Data Interface), permite reducir considerablemente el coste de las conexiones.

Las distancias son claramente más cortas: de una treintena a un centenar de metros, dependiendo de la calidad de los pares metálicos.

TPDDI puede descomponerse en dos subclases:

- TPDDI sobre STP (Shielded Twisted Pair), para la utilización de FDDI sobre pares trenzados blindados.

Algunas sociedades, como Cabletron, Chipcom y Synoptics especialmente, ya se han inclinado hacia la realización de tarjetas de este tipo. Estas tarjetas permiten la comunicación a 100 Mbits/s sobre un cable de par trenzado blindado

.

- TPDDI sobre UTP (Unshielded Twisted Pair), para la utilización de FDDI sobre pares trenzados sin blindar.

Se han hecho algunos pronunciamientos referentes a la realización de una red FDDI sobre este tipo de pares. AT&T, Apple Computer, Cabletron, Fibronics y Ungermann-Bass -que incluso se han asociado en un grupo llamado UTPF (Unshielded Twisted Pair Foundation)-, con el fin de

CODESIS COMERCIALIZADORA EDITORIAL Y SISTEMAS LTDA.

potenciar los productos FDDI sobre UTP.

De esta forma, cabría esperar al menos dos normas ANSI relativas a la FDDI sobre pares trenzados: la primera para la utilización del par trenzado blindado (tipo 1 y 2 de IBM); la segunda para el par trenzado sin blindar, previsto para distancias inferiores a 100m.

REDES QUE UTILIZAN LAS FIBRAS ÓPTICAS

FDDI

INTRODUCCIÓN

FDDI (Fiber Distributed Data Inteface) hacia 1980, comienzan a necesitarse redes que transmitan datos a alta velocidad. También se necesitaba transmitir datos en tiempos cortos y acotados. En respuesta a estas necesidades, se desarrolla FDDI. FDDI ofrece 100 Mbps, con hasta 500 estaciones conectadas y un máximo de 100 km. entre ellas. Las estaciones se conectan en un doble anillo de fibra óptica por seguridad. Por su alta velocidad de transmisión, también puede usarse como una red de conexión entre redes más pequeñas.

FUNCIONES DE FDDI

Las funciones de FDDI se definen en el SMT (Station ManagemenT). Abarcan la capa física (PMD y PHY) y parte de la capa de enlace (MAC).

Por ello, FDDI se instala en los niveles más bajos de la torre OSI. No habría problemas en usar otros protocolos para las capas superiores, en principio. Por contra, las implementaciones sólo han conseguido encapsular correctamente ARP e IP sobre FDDI.

EL NIVEL FÍSICO:

PMD

En el nivel dependiente del medio (PMD), FDDI no impone restricciones al tipo de fibra que debe usarse. Puede utilizarse fibra multimodo (MMF), o fibra monomodo (SMF).

Las fibras serán de dimensiones 62,5/125 o 85/125 (diámetro del núcleo/diámetro de la fibra). MMF necesita mejores emisores y receptores que SMF para mantener las mismas longitudes de enlace.

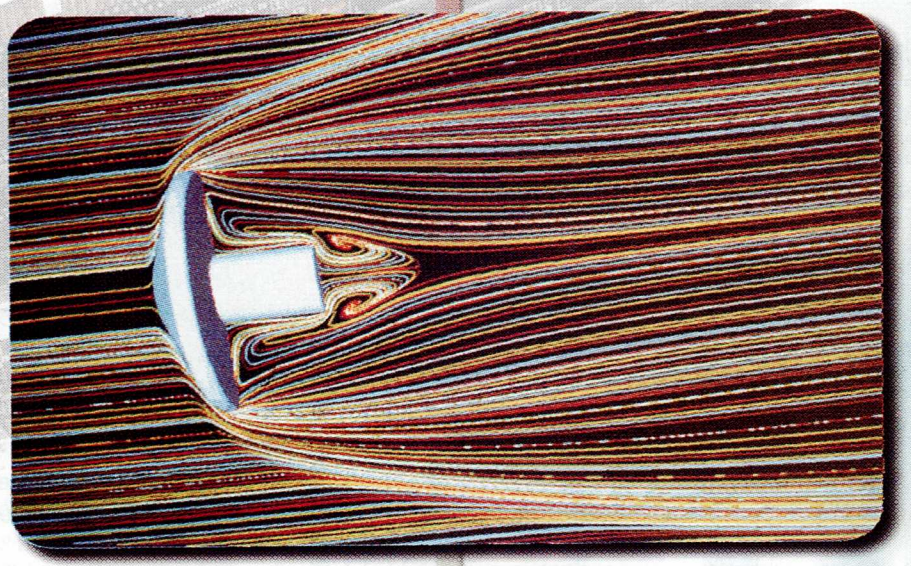
En cualquier caso, la potencia de transmisión mínima es de -16 dBm y la potencia recibida mínima es de -26 dBm, lo que deja un margen de 11 dBs para pérdidas. Los transmisores pueden ser LED o láseres. Los receptores pueden ser diodos PIN o de avalancha. Se trabaja en la ventana de 1300 nanómetros.

En una misma red puede haber enlaces con fibras MMF y SMF, aunque deben examinarse con cuidado. Se recomienda emplear conectores SC preferentemente. También pueden emplearse conectores ST. La probabilidad de error requerida es 4*10-11.

NIVEL FÍSICO:

PHY

El otro subnivel físico, PHY, define el protocolo de introducción de datos en la fibra. FDDI introduce redundancia en los datos en transmisión.



Un haz de fibras ópticas puede transformar miles de conversaciones telefónicas y decenas de canales de televisión.

Usa un código 4B/5B, transmite 5 bits por cada 4 bits que le envía el nivel superior.

La elección de los códigos se hizo para equilibrar la potencia en continua del código, y evitar secuencias de 0's o 1's demasiado largas. El régimen binario efectivo que soporta la fibra es de 125 Mbps.

MAC define la longitud máxima de trama en 4500 bytes para evitar problemas de desincronización. No hay longitud de trama mínima. El formato de trama es:

PA = Preámbulo: 30 caracteres IDLE, para sincronismo.

SD = delimitador de inicio. No se repite en el campo de datos.

FC = control de trama. Tipo de trama (síncrona, ...).

DA = Dirección de destino.

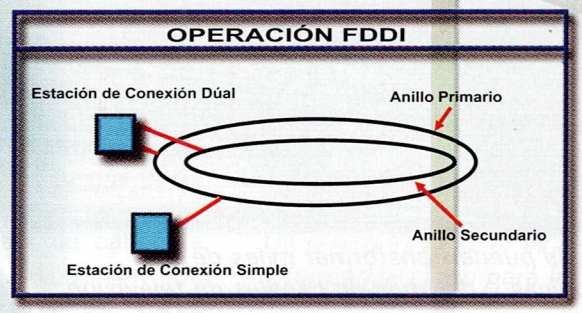
SA = Dirección de destino.

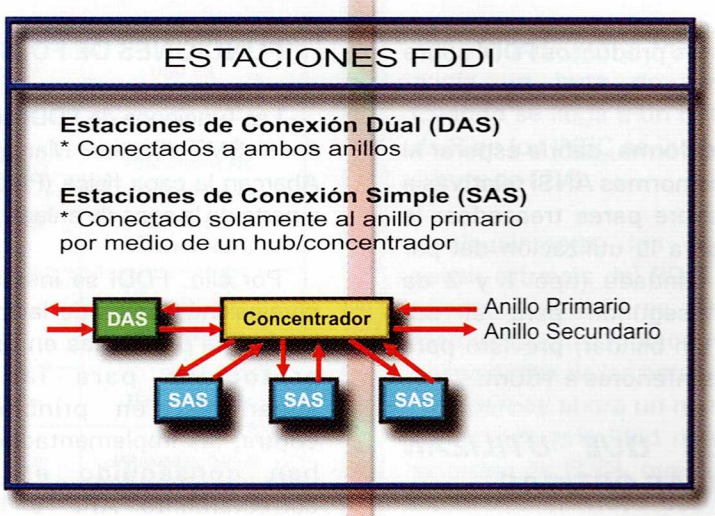
INFORMACION: Datos transmitidos.

FCS = Redundancia de la trama con CRC-32.

ED = Delimitador de fin de trama. No se puede repetir en el campo de datos.

FS = Frame Status. Receptor informa a origen del resultado de la trama (trama errónea, bien recibida, ...)





Una estación que está transmitiendo trama debe retirarla del anillo. Mientras lo hace, puede introducir nuevas tramas, o transmitir caracteres IDLE, hasta retirarla completamente.

Dado que protocolos superiores (UDP, por ejemplo) definen longitudes de trama diferentes, las estaciones deben estar preparadas para fragmentar/ensamblar paquetes cuando sea necesario.

NIVEL DE ENLACE:

MAC

MAC aporta las mayores novedades de FDDI. FDDI soporta dos tipos de tráfico:

- Tráfico síncrono: voz, imágenes, información que debe ser transmitida antes de un determinado tiempo.

Podría decirse que es tráfico de datos en tiempo real.

- Tráfico asíncrono: e-mail, ftp, información para la cual el tiempo que tarde en llegar al destino no es el factor decisivo.

La filosofía que persigue FDDI es atender primero el tráfico síncrono y después el tráfico asíncrono. Para ello, cada estación tiene varios temporizadores:

- Token Rotation Time (TRT): tiempo transcurrido desde que llegó el último testigo.

- Token Hold Time (THT): tiempo máximo que una estación puede poseer el testigo.

Todas las estaciones tienen un parámetro fijo, el Target Token Rotation Time (TTRT), que fija el tiempo que tarda el testigo en dar una vuelta al anillo, y cada una tiene un parámetro propio, Syncronous Time (ST o Ci, dependiendo de autores). Este parámetro fija el tiempo máximo que una estación está transmitiendo tráfico síncrono.

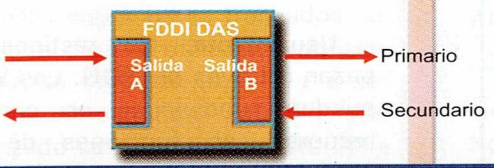
El mecanismo que se sigue es el que se muestra en el siguiente diagrama de flujo :

1) Cuando llega el testigo, comprobamos que ha llegado a tiempo. Para ello, vemos si TRT > 0.

CODESIS COMERCIALIZADORA EDITORIAL Y SISTEMAS LTDA.

PUERTOS FDDI

* **DAS A** - Primario Entrada, Secundario Salida.
* **DAS B** - Primario Entrada, Secundario Salida.
* **Dueño** - Puerto concentrador solamente.
* **Esclavo** - SAS sólo primario de entrada y de salida



Si es cierto, la estación captura el testigo. Si es falso, la estación lo deja pasar a la siguiente estación. En cualquier caso, TRT se reinicializa a TTRT.

2) Una vez la estación posee el testigo, el valor de TRT se carga en THT. Se comienzan a transmitir tramas síncronas.

3) THT llega a cero. En ese caso, se termina el turno de la estación, y se pasa el testigo a la siguiente.

4) Antes de que THT llegue a 0 se acaban las tramas síncronas que tenía la estación preparada para transmitir. Se transmiten ahora todas aquellas tramas asíncronas de que se dispongan, hasta que THT llegue a cero.

5) Si acabamos también las tramas asíncronas, pasamos el testigo.

Se plantea un problema cuando se acaba el THT mientras se está transmitiendo una trama. Este fenómeno se llama overrun. El intervalo máximo entre dos testigos en una estación ronda 2*TTRT. Las estaciones se conectan mediante un doble anillo de fibra óptica. En cada anillo, la información circula en una dirección.

En caso de que caiga un enlace entre dos estaciones, las fibras se puentean internamente en las estaciones, de modo que el anillo no se para. Esta configuración clasifica las estaciones en dos clases:

- **DAS** : **Dual Attachment Station**. Estación conectada al doble anillo. Capaces de reconfigurarse. Más caras.

- **SAS** : **Single Attachment Station**. Estación conectada a uno de los dos anillos solamente. Más baratas.

OTRAS SOLUCIONES ALTERNATIVAS

Se han planteado otras soluciones al estándar original expuesto anteriormente. Todas las soluciones se basan en el estándar FDDI, aunque varían algunos niveles, para adaptarlo a determinadas situaciones.

Las soluciones más atractivas son CDDI, FDDI-II, y LCF-FDDI

CDDI

CDDI (Copper Distributed Data Interface) no es otra cosa que FDDI utilizando cables de cobre en lugar de fibra óptica como medio de transmisión. Sólo afecta al PMD. Para seguir cumpliendo los requerimientos de ruido y velocidad de transmisión se reduce la distancia máxima de enlace a 100 m. Para evitar también la radiación que produce el par trenzado sin blindaje (Unshielded Twisted Pair, UTP) cuando se utilice este medio de transmisión se utiliza un código diferente, NRZ- III.

Básicamente, es NRZ con tres niveles, subiendo y bajando niveles hasta llegar a los extremos. De este modo, baja la frecuencia máxima que soporta el par trenzado, reduciéndose las radiaciones.

La principal ventaja que aporta CDDI es la reducción en los costes de implantación de FDDI, sobre Todo cuando se quiere hacer llegar FDDI hasta los terminales de usuario (FDDI- on-desk).

Todo cuando se quiere hacer llegar FDDI hasta los terminales de usuario (FDDI- on-desk). Los terminales suelen estar ya cableados, por lo que sustituir el cobre por la fibra óptica aparece como un coste innecesario en muchos casos.

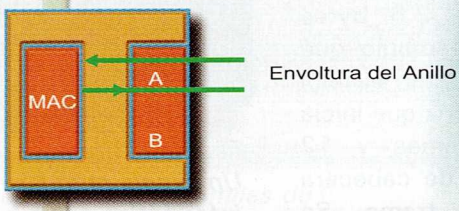
Además, los receptores y transmisores ópticos que emplea FDDI resultan demasiado caros frente a los dispositivos electrónicos que utiliza CDDI.

Por lo demás, los cambios en el código no son relevantes y la reducción en la distancia máxima no es importante, puesto que CDDI

INTERRUPTOR DERIVANTE ÓPTICO

* Cuando una estación se desconecta pasa a un modo de derivante.

* Evita la envoltura del anillo.



BANDA DE FRECUENCA	DESIGNACION	LONGITUD DE ONDA	USO EN COMUNICACIONES
300KHz → 3 Mhz	MF (Middle frecuency)	1Km → 100m	Radiodifusión AM
3KHz → 30 Mhz	HF (High Frecuency)	100m → 10m	Onda Corta (radioaficionados)
30KHz → 300MHz	VHF 8 Very High Frecuency)	10m → 1m	TV, Radio FM, Radiollamadas
300KHz → 3GHz	UHF (Ultra High frecuency)	1m → 10Cm	Microondas, TV.
3GHz → 30GHz	SHF (Super High Frecuency)	10Cm → 1Cm	Microondas, Satélite

Relación de bandas y designación de las mismas

se utilizaría dentro de los edificios, en los que las distancias suelen ser inferiores a esos 100 metros críticos.

FDDI-II

FDDI-II cambia el servicio que ofrece. Amplía SMT hasta completar el nivel de enlace. Ahora el nivel de red no ve un único canal de 100 Mbps sino que este canal se divide en 16 canales síncronos de 6,144 Mbps (WBC), y un canal de transmisión de paquetes, de 768 Kbps (PDG).

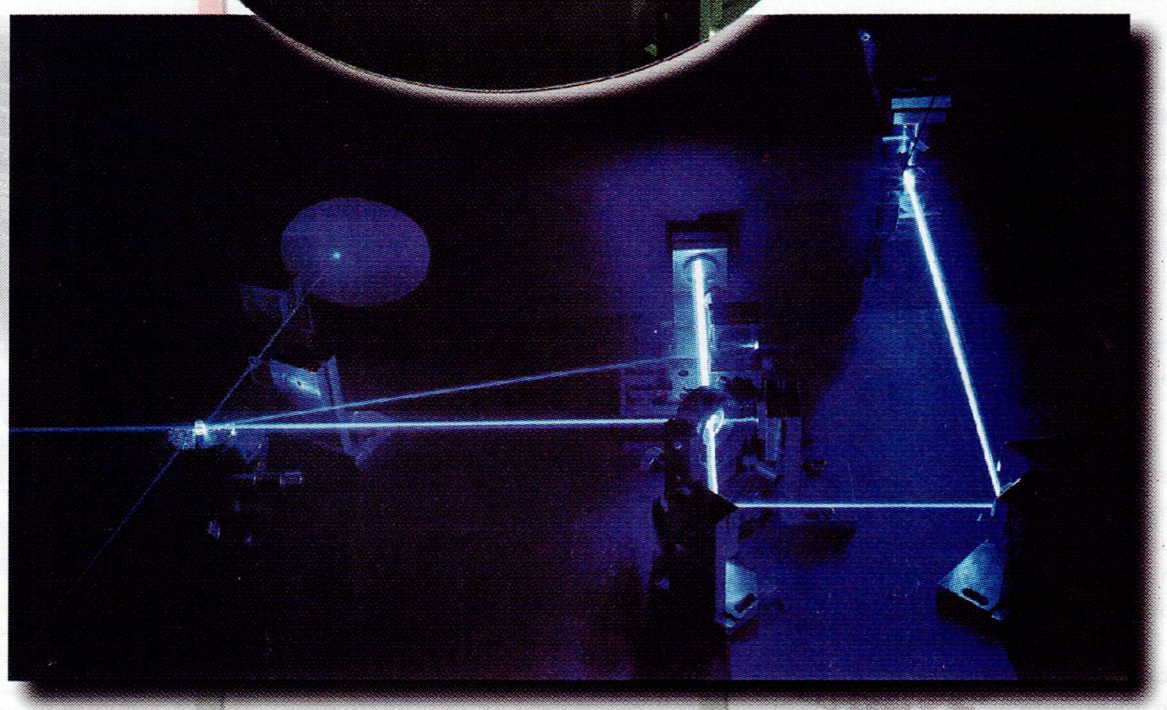
Las tramas son de 0.125 ms y contienen intercalados los distintos canales. Inicialmente, se envían 2,5 bytes de preámbulo que sincronizan el reloj de 8 Khz que inicia las tramas y 12 bytes de cabecera de la trama. Se envía el byte correspondiente al PDG. Luego se envía un byte de cada canal. Cuando se llega a un byte múltiplo de 8 en los WBC se vuelve a enviar 1 byte de PDG.

Usualmente, los testigos se pasan a través del PDG. Los WBC pueden subdividirse en canales menores, en funciones de las necesidades de las estaciones.

Aparece ahora un nuevo tipo de tráfico, de prioridad mayor que el síncrono de FDDI, que es el tráfico conmutado. Hay dos testigos, testigo restringido y testigo sin restricciones. Dependiendo de las restricciones en tiempo de llegada de las tramas se utiliza una combinación de tráfico y testigos.

LCF-PMD

LCF-PMD (Low-Cost Fiber Physical Medium Dependent) surge



El uso de fibras ópticas para emitir señales está muy extendido. Un simple rayo láser es capaz de contener una gran cantidad de información tanto para la informática como para las telecomunicaciones

CODESIS COMERCIALIZADORA EDITORIAL Y SISTEMAS LTDA.

también como ante necesidad económica. Se busca reducir el coste de implantación de una red FDDI. Para ello, se cambia de nuevo el PMD.

Se introducen nuevos tipos de fibra (200/230), más baratos y de peores prestaciones. Igual que en CDDI, se amplían los márgenes de ruido, y se reducen las longitudes de los enlaces, ahora hasta los 500 metros.

Se reduce la potencia mínima de transmisión en 2 dBm. Se relaja en 2 dBm la potencia mínima de recepción, quedando sólo 7 dBs para pérdidas. El resto del protocolo no se altera.

Rendimiento

El rendimiento de FDDI se mide en dos aspectos: Retardo de las tramas en llegar a la estación destino y cantidad de datos que llegan a destino por segundo. Un primer parámetro de importancia es el TTRT.

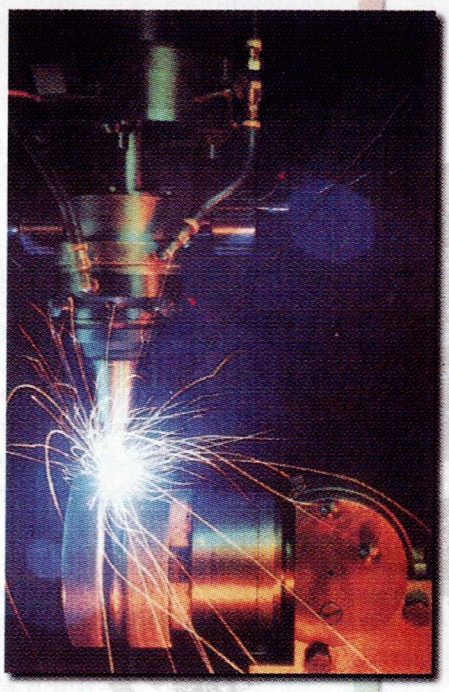
Si es pequeño, el testigo circula muy rápidamente, de modo que el retardo es pequeño. Si es grande, el throughput es mayor, pero estaciones con mucha carga retrasan a las demás. Los valores típicos de TTRT rondan los 4 ms, según [2] o los 165 ms, según [6]. Otro factor a tener en cuenta es el tamaño de los paquetes. Si es grande, aumenta el throughput. Si es pequeño, disminuye el retardo.

Conclusiones

En conclusión, FDDI ofrece transmisión de datos a alta velocidad, en tiempo real o no, entre un número de estaciones alto y separadas una distancia elevada. También puede servir como red de conexión entre LANs que están funcionando previamente. Se ha sabido adaptar a las características de entornos en los que resulta muy deseable disponer de ella, pero su elevado coste inicial parecía prohibir. Esto hace de FDDI y LCF alternativas muy interesantes para LANs.

Sin embargo, la irrupción de ATM ha hecho que FDDI se considere "la hermana pequeña" de las redes de comunicación óptica.

ATM ha hecho que FDDI ya no sea un campo de investigación tan activo como fue a finales de los 80, ni siquiera en FDDI-II, que aprovecha parte de las ideas que utiliza las ideas de ATM. Por ejemplo, la inclusión de canales virtuales conmutados.



Las fibras ópticas se pueden utilizar tanto para transmisión de imágenes como para comunicaciones.

MODELOS DE PROPAGACIÓN.

PROPAGACIÓN DE LAS ONDAS ELECTROMAGNÉTICAS

Las ondas electromagnéticas son literalmente impulsos eléctricos que se desplazan por el medio ambiente.

Su descubrimiento se debe al científico Heinrich Hertz, por esta razón, las ondas electromagnéticas se conocen con el nombre de ondas de radio o hertzianas. Son bastante similares a las ondas de luz, ya que ambas poseen características electromagnéticas

ESPECTRO DE RADIOFRECUENCIAS

El espectro de radiofrecuencias hace referencia a cómo está dividido todo el ancho de banda que se puede emplear para transmitir diversos tipos de señales. Existe una reglamentación que asigna determinadas frecuencias a determinados tipos de transmisión de información .

Los campos eléctrico y electromagnético son perpendiculares entre sí y perpendiculares a la dirección de propagación.

FENÓMENOS:

- **Reflexión** (Obstáculos)
- **Refracción** (Diferentes capas de la atmósfera).
- **Difracción** La onda electromagnética al pasar junto al

borde de un objeto opaco cambia de trayectoria.

ATENUACIÓN

MODELOS DE PROPAGACIÓN

- **Ondas de Superficie (VLF - HF)**

El frente de ondas se va curvando hasta que se cortocircuita con la tierra. No puede atravesar obstáculos. Se necesitan antenas muy grandes (de orden landa).

- **Ondas del Cielo (HF)**

Sirven para comunicar puntos muy lejanos entre sí. Las ondas se refractan al atravesar la ionósfera y vuelven a la tierra. Si el ángulo de incidencia con la ionósfera es muy grande la onda se puede perder en el espacio.

- **Ondas del Espacio (VHF-UHF)**

Se propagan en línea recta, fenómenos de reflexión y refracción con obstáculos.

- **Ondas Troposféricas (SHF)**

Se propagan a 15 Km de la superficie. 1/5 Ghz.

NORMATIVA DE INTERCONEXIÓN.

La veremos con los distintos tipos de multiplexación

- **Multiplexión en tiempo en recepción y emisión:**

Las estaciones dentro de un área emiten en intervalos de tiempos separados. En recepción el satélite incorpora información indicando a qué estación va destinada.

- **Multiplexación por división de frecuencias:**

A través del medio todas las estaciones transmiten simultáneamente pero en un rango de frecuencias diferente.

Multiplexación en frecuencia para recepción y multiplexado en tiempo para emisión. Permite una mejor separación entre canales.

NATURALEZA DE LAS ONDAS DE RADIO

El proceso de transmisión es el siguiente: Se aplica una potencia de radiofrecuencia a una antena (una potencia eléctrica modulada). Los electrones contenidos en el metal de la antena, comienzan a oscilar instantáneamente.

El movimiento de estos electrones genera una corriente eléctrica que se manifiesta de dos formas sobre la antena.

Mediante un campo magnético concéntrico al conductor de la antena, con líneas de fuerza concéntricas al conductor, y un campo electrostático cuyas líneas de fuerza son perpendiculares a las líneas de fuerza del anterior campo, es decir centrífugas.

La fuerza o potencia eléctrica que se aplica a la antena tiene una forma senoidal, forma que fielmente reproducen tanto las ondas magnéticas como las electrostáticas.

La longitud de onda está directamente relacionada al tamaño de la antena, aspecto que debe ser considerado al momento de instalar la misma.

La fibra óptica permite tambien examinar zonas inaccesibles por inspección directa en el sector mecánico. En comunicaciones, la fibra óptica es más eficaz, y ligera,y menos voluminosa y cara que los hilos de cobre.

CODESIS COMERCIALIZADORA EDITORIAL Y SISTEMAS LTDA.

1) El servidor determina primero si el nombre y la contraseña del usuario son correctos.

2) Si lo son, aparece el cuadro de diálogo **Devolución de llamada** en el equipo del usuario.

3) El usuario escribe el número de devolución de llamada en el cuadro de diálogo y espera que el servidor le llame.

Sin devolución de llamada

Si la cuenta de usuario no se ha configurado para devolución de llamada, **RAS** establece una conexión tan pronto como se autentifican el nombre y la contraseña del usuario.

Compatibilidad de hosts y conmutadores de seguridad

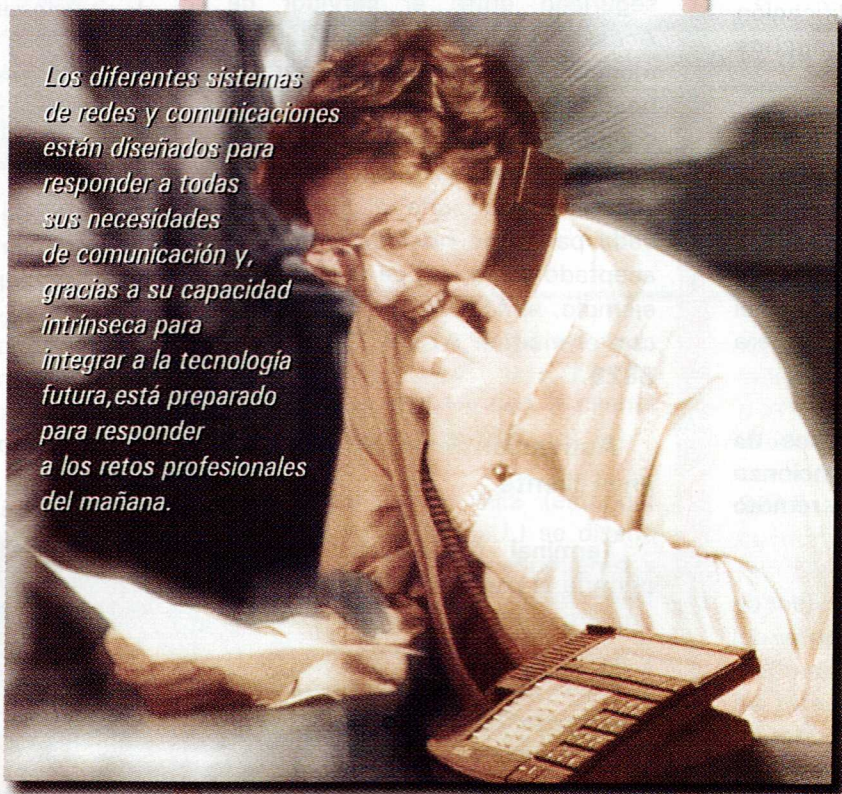
RAS acepta varios tipos de dispositivos intermedios (hosts y conmutadores de seguridad) entre el cliente de **Acceso remoto** y el **servidor de Acceso remoto**.

Entre dichos dispositivos se incluyen:

- Conmutador de banco de modems.
- Un host de seguridad.
- La red X.25

Conexión a través de dispositivos intermedios

Antes de conectar con el **servidor de Acceso remoto**, un cliente puede tener uno de estos dos posibles diálogos (entradas del usuario y pantallas de respuesta del equipo) con cada dispositivo intermedio:



Los diferentes sistemas de redes y comunicaciones están diseñados para responder a todas sus necesidades de comunicación y, gracias a su capacidad intrínseca para integrar a la tecnología futura, está preparado para responder a los retos profesionales del mañana.

- **Estático** (un diálogo que es siempre igual y no requiere entrada por parte del usuario).
- **Interactivo** (un diálogo que cambia siempre, requiriendo entrada por parte del usuario).

Tiene que configurar el cliente para que opere con cada dispositivo intermedio.

Si necesita diálogos estáticos e interactivos, tiene que ejecutar dos acciones:

1) Escribir un archivo de comandos para el diálogo estático. (Consulte la siguiente sección, "**Escritura de archivos de comandos**".).

2) Activar el modo terminal para los diálogos interactivos. (Consulte "**Activación del modo terminal en el cliente**", más adelante en este mismo capítulo.).

Si sólo necesita un tipo de diálogo, ejecute sólo uno de los pasos anteriores. Por ejemplo:

- Si sus clientes se conectan solamente a través de un dispositivo intermedio con un diálogo estático (como una red X.25), omita el paso 2.
- Si sus clientes se conectan a través de un host de seguridad con un diálogo interactivo, omita el paso 1.

Escritura de archivos de comandos

La figura es un ejemplo de la necesidad de dos diálogos: preconexión (un conmutador de banco de modems) y postconexión (un host de seguridad).

Aunque los diálogos de preconexión y postconexión pueden ser estáticos o interactivos, el diálogo de preconexión es normalmente estático y el de postconexión es normalmente interactivo.

En los diálogos estáticos, el usuario selecciona un archivo de comandos personalizado en el cuadro de diálogo **Switch**. En los diálogos interactivos, el usuario selecciona **Terminal** en el cuadro de diálogo **Switch**.

El archivo **SWITCH.INF** incluido en **Windows NT** proporciona un archivo de comandos genérico que funcionará seguramente con pequeñas o ninguna modificación cuando conecte con muchos servidores **PPP**.

Intente conectarse usando el archivo de comandos genérico. Si esto no funciona, puede copiar y modificar el archivo de comandos genérico para adaptarlo a la secuencia de inicio de sesión del equipo remoto al que se quiera conectar.

Para que los dispositivos de seguridad de terceros funcionen con el Servicio de Acceso remoto siga los siguientes pasos

1) Si el módem del **servidor de Acceso remoto** es diferente del incluido en la sección de módem del host de seguridad en **Modem.inf**, el archivo **Modem.inf** del **servidor de Acceso remoto** se debe personalizar para vincular el **host de seguridad** con el módem del servidor.

2) El usuario remoto tiene que activar el modo **Terminal** para interactuar con el **host de seguridad**.

Para poder utilizar un **host de seguridad** de **Security Dynamics**, tiene que pedir dos conectores a su proveedor de **Security Dynamics** para permitir la inicialización del módem **RAS**. Al hacer el pedido, especifique que desea la opción de marcado.

El proveedor le enviará una puerta **AND** y una caja con puentes. Para el host de seguridad **ACM/400**, también recibirá software diferente.

Personalización del archivo Modem.inf en el Servidor de acceso remoto

Cuando instale un **host de seguridad** entre el **servidor de Acceso remoto** y su módem o modems, el módem del servidor y el **host de seguridad** actúan de forma conjunta como un nuevo tipo de módem. El archivo **Modem.inf** se suministra con una plantilla para cada pareja de **host de seguridad** aceptado y módem particular. (Por ejemplo, el **ACM/400** forma pareja con el módem **AT&T® Comsphere 3820.)**

Activación del modo Terminal en el cliente

Terminal de Acceso remoto permite al usuario remoto enviar el número de acceso adecuado al dispositivo de seguridad. Si el número es correcto, el usuario queda conectado con el **servidor de Acceso remoto.**

Auditoría

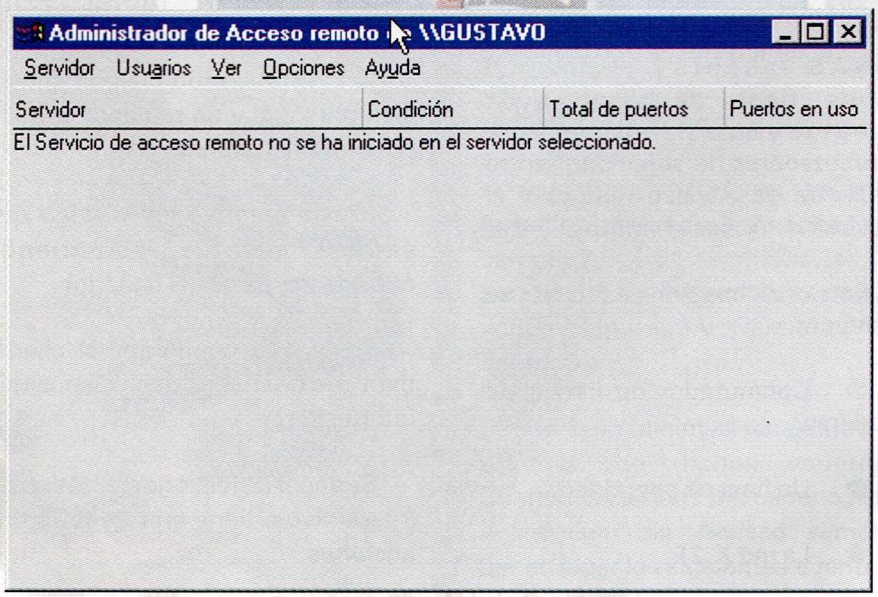
RAS genera registros de auditoría para las conexiones remotas. Con esta característica, puede auditar la actividad de Acceso remoto utilizando el **Visor de sucesos de Windows NT Server** para comprobar que la seguridad de la red se mantiene intacta. También puede monitorizar los servidores y los usuarios con el **Administrador de acceso remoto.**

Mantenimiento y solución de problemas

Una vez que haya instalado el **Servicio de acceso remoto**, su mantenimiento rutinario consiste en las siguientes tareas:

- Monitorizar sistemáticamente los servidores y usuarios con **Administrador de acceso remoto.**
- Revisar con regularidad el **Visor de sucesos de Windows NT Server** para ver si la seguridad de la red está intacta.

El programa **Administrador de Acceso remoto**, mediante la comunicación de información en



CODESIS COMERCIALIZADORA EDITORIAL Y SISTEMAS LTDA.

tiempo real referente a usuarios, puertos, modems y transmisiones de datos, simplifica la monitorización de los servidores y usuarios, y proporciona valiosas indicaciones para ayudar a resolver problemas.

Si deja el programa activado continuamente, podrá hacer un seguimiento de la actividad en sus **servidores de Acceso remoto** y responder puntualmente a los problemas con las cuentas de usuarios y el hardware.

Con el programa **Administrador de Acceso remoto**, puede ver el dominio del **Servicio de acceso remoto** de dos modos:

a) Los **servidores de Acceso remoto** dentro de un dominio. Esta perspectiva del dominio le permite administrar múltiples **servidores de Acceso remoto** desde un lugar centralizado.

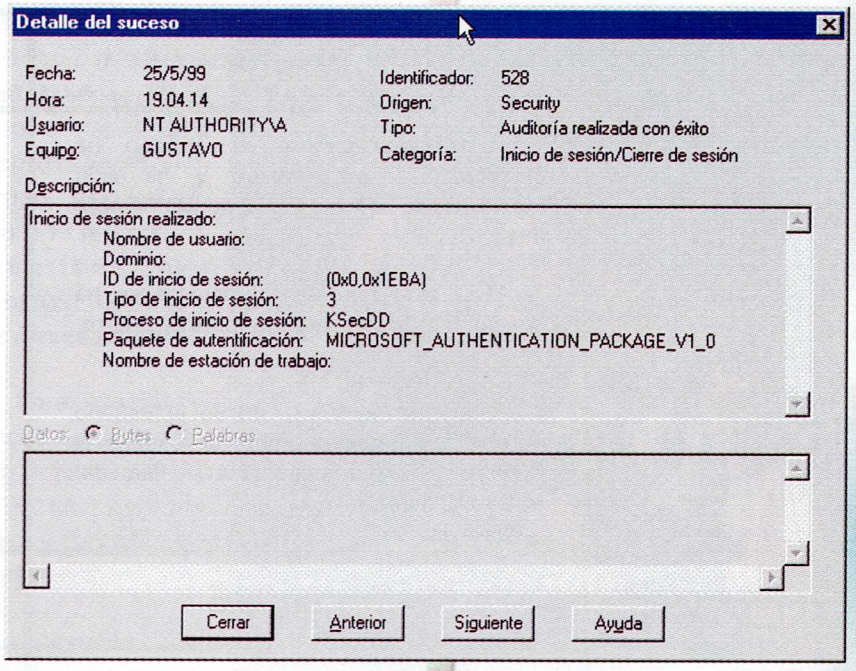
b) Todos los usuarios que están conectados a esos servidores.

Esta perspectiva le permite monitorizar la actividad de los usuarios en todos los **servidores de Acceso remoto del dominio**.

La ventana **Administrador de acceso remoto** muestra un único servidor **RAS** o todos los servidores **RAS** de un dominio. La vista predeterminada es lo que vio por última vez.

Puede cambiar el enfoque a otro dominio diferente o bien puede concentrarse en un único servidor del dominio actual.

El programa **Administrador de acceso remoto** requiere que el usuario haya iniciado una sesión como **Administrador**.



La utilidad **Administrador** proporciona información en tiempo real acerca de los usuarios activos y las conexiones actuales y, por tanto, es el punto de partida apropiado para empezar a resolver problemas. Considere los siguientes ejemplos de uso de este programa:

- Quizá observe en la ventana **Administrador de acceso remoto** que en un servidor se usa constantemente un número menor de puertos del que se esperaba, lo que sugiere que uno o varios puertos no están funcionando adecuadamente.

- Si los usuarios no pueden establecer una conexión, puede pedirles que intenten establecer una nueva conexión mientras usted monitoriza sus intentos en el cuadro de diálogo **Estado del puerto**.

Cuando los datos en tiempo real no son suficientes para resolver un problema, puede consultar las auditorías y los mensajes de error generados por **Acceso remoto**.

El **Visor de sucesos de Windows NT Server** registra todas las auditorías y mensajes de error de Acceso remoto.

ADVERTENCIA

Condición irregular o inesperada que no afecta a la funcionalidad del sistema.

Los sucesos se clasifican en tres categorías principales:

Descripción del Suceso

Auditoría Comportamiento normal registrado para la administración, por ejemplo, información acerca de un cliente conectado: nombre del usuario, tiempo de conexión y estado actual.

Error Fallo grave de una función o un error en la red.

Las auditorías se dividen a su vez en dos categorías:

	MENSAJE	EXPLICACIÓN
ACCESO CORRECTO AUDITADO	El usuario nombre de usuario ha establecido una conexión y ha sido autentificado con éxito en el puerto nombre de puerto.	Este mensaje significa una conexión normal realizada por un usuario en un puerto determinado.
	El usuario nombre de usuario se ha desconectado del puerto nombre de puerto.	Este mensaje registra una desconexión con éxito iniciada por el usuario.
	Se ha devuelto la llamada al usuario nombre de dominio\nombre de usuario al número número de devolución de llamada, por puerto número.	Este mensaje indica una correcta devolución de la llamada a un usuario en el número de teléfono especificado.
	MENSAJE	**EXPLICACIÓN**
ACCESO ERRÓNEO AUDITADO	El usuario conectado al puerto nombre de puerto ha sido desconectado debido a inactividad.	La línea ha estado libre por un período de tiempo superior al configurado usando el parámetro AutoDisconnect en el Registro.
	El usuario ha establecido una conexión y no fue autentificado en el puerto nombre de puerto. La línea ha sido desconectada.	El usuario ha suministrado un nombre de usuario, una contraseña o ambos incorrectos. El número de autentificaciones incorrectas antes de que se niegue el acceso y se corte la línea depende del valor del parámetro AuthenticateRetries del Registro.
	El usuario conectado al puerto nombre de puerto ha sido desconectado debido al tiempo de espera de la autentificación.	La autentificación tomó más tiempo que el establecido. Puede que necesite aumentar el valor del parámetro AuthenticateTime.
	El usuario conectado al puerto nombre de puerto ha sido desconectado porque ha habido un error en el nivel de transporte durante la conversación de autentificación.	Han ocurrido demasiados errores durante la conversación de autentificación, posiblemente debido a líneas ruidosas o modems no compatibles. Pídale al usuario que intente conectarse con una velocidad inicial menor.
	El usuario conectado al puerto nombre de puerto ha sido desconectado debido a que no ha podido ser proyectado en la red.	Lo más probable es que el nombre de equipo del usuario ya exista en la red. Pídale al usuario que configure el equipo remoto con un nombre distinto o que se asegure de que el equipo no está conectado actualmente a la red por otros medios, como Ethernet o Token Ring.

CUADRO 4

CODESIS COMPEDIALIZADORA EDITORIAL Y SISTEMAS LTDA.

Categoría de la auditoría

Acceso correcto auditado

Un cliente establece una conexión y se desconecta normalmente.

Acceso erroneo auditado

El servidor corta la conexión de un cliente que ha estado inactivo por mucho tiempo o un cliente intenta establecer una conexión con la contraseña equivocada.

Auditorías

El **Visor de sucesos de Windows NT Server** registra la actividad de cada **servidor de Acceso remoto**. Puesto que las auditorías que se registran en el **Visor de sucesos** son la mejor evidencia de posibles intentos de infringir la seguridad de la red, asegúrese de revisarlas con regularidad.

El **Servicio de acceso remoto** genera, entre otros, los siguientes registros de auditorías: CUADRO 4

NOTA

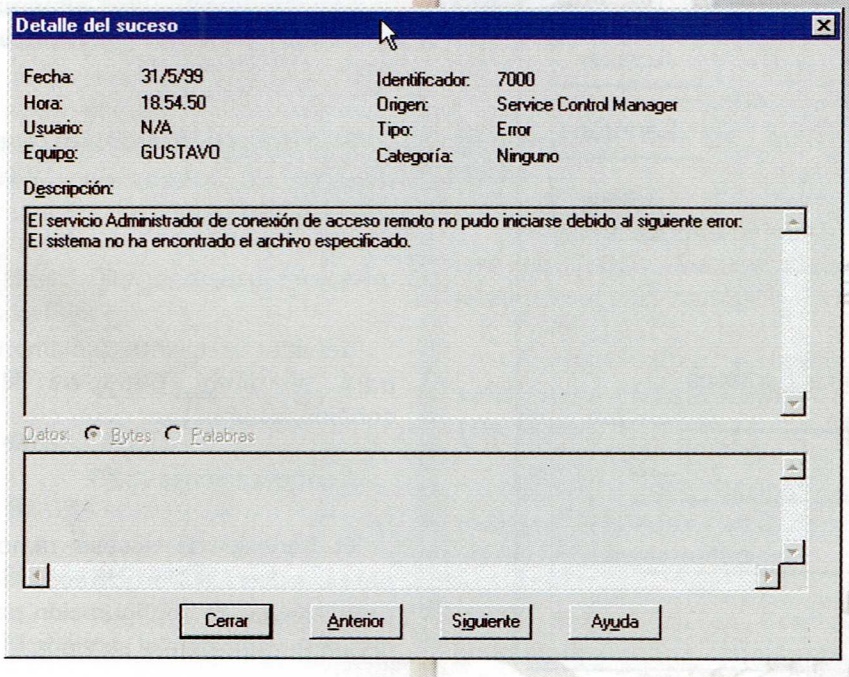
Si no es posible iniciar el Servicio de acceso remoto, consulte el Visor de sucesos para buscar una descripción del error ocurrido.

Puesto que los problemas del cliente generalmente provienen de configuraciones erróneas del software o hardware en el equipo, compruebe primero el mensaje de error y los registros de auditoría para encontrar algunas indicaciones.

Registros específicos de RAS

Para activar dos registros específicos de **RAS** (el registro **PPP** y el registro de dispositivo), cambie algunos parámetros en el **Registro**.

Estos registros son archivos de texto que pueden verse en cualquier editor de texto o en la interfaz de comandos.

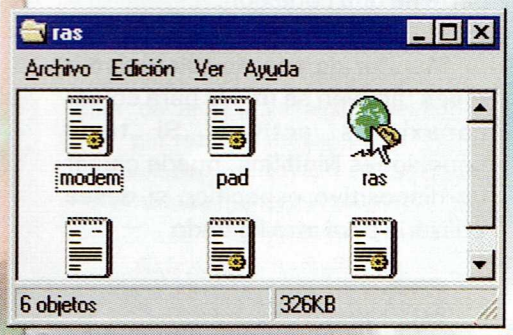


Los registros no se pueden examinar en el **Visor de sucesos**.

El registro PPP

Cuando está activado, el registro **PPP** graba todos los sucesos de **PPP** en el archivo **\raíz_sistema\SYSTEM32\RAS\PPP.LOG**. Este archivo de registro resulta útil para determinar posibles problemas con las conexiones de **PPP**. Para activar el registro **PPP**, vaya a la siguiente clave y cambie a 1 el parámetro **Logging**:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP



El registro de dispositivo

Cuando está activado, el registro de dispositivo se crea en el archivo **\raíz_sistema\SYSTEM32\RAS\DEVICE.LOG**. Este registro graba todas las comunicaciones realizadas desde los puertos serie en el dispositivo conectado a ellos durante la modalidad de comandos.

El proceso de registro se detendrá cuando se haya completado con éxito la conexión al dispositivo y se transmitan datos. Para activar el registro de dispositivo, vaya a la siguiente clave y cambie a 1 el parámetro Logging:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters

Informe de estado

El **Monitor de acceso telefónico a redes** (situado en el Panel de control) proporciona el estado de una llamada y le permite ver:

- La velocidad con la que se ha conectado.
- La duración de la conexión.
- Los nombres de los usuarios conectados a un servidor **RAS**.
- Los protocolos usados durante la conexión.
- Qué dispositivos forman parte de una conexión.

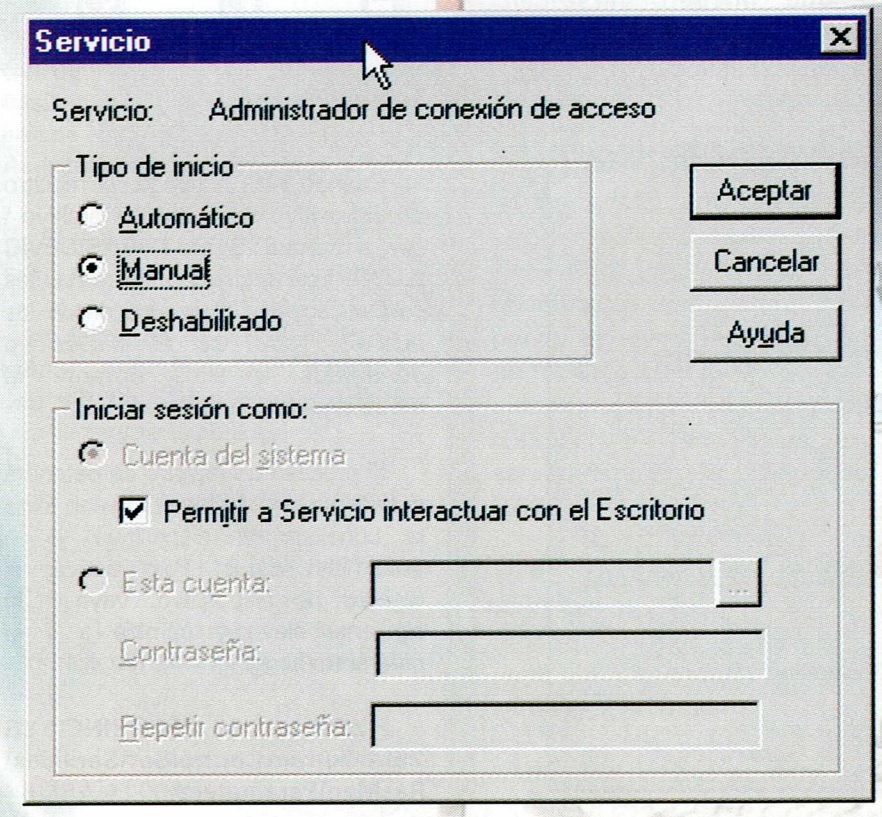
Monitor de acceso telefónico a redes también se utiliza para colgar conexiones activas. Si tiene conexiones **Multilink**, puede colgar un dispositivo específico si desea utilizarlo para otra llamada.

De forma predeterminada, **Monitor de acceso telefónico a redes** aparece en la barra de tareas a medida que usted marca al exterior.

Utilice la ficha **Preferencias** para cambiar la vista y configurarla para que aparezca como una ventana. **Monitor de acceso telefónico a redes** presenta luces para indicar tráfico a través de las líneas telefónicas: un botón azul intermitente cuando se envían o reciben datos y un botón rojo intermitente cuando se produce un error.

Administrador de acceso remoto

Además, cuando **Monitor de acceso telefónico a redes** se ve como una ventana, puede configurarlo para mostrar filas de luces para múltiples dispositivos. Para ello, en la ficha **Preferencias**, haga click en **Luces**.



Compatibilidad con PAD X.25

Una red **X.25** utiliza un protocolo de conmutación de paquetes para transmitir datos. Este protocolo depende de una red mundial compleja de nodos de reenvío de paquetes (Equipo de comunicaciones de datos, **DCE**) que participan en la entrega de un paquete **X.25** a su dirección designada.

Los Ensambladores / **desensambladores de paquetes (PAD)** asíncronos de marcado constituyen una elección práctica para los clientes de **Acceso remoto** ya que no requieren una línea X.25 para poder enchufarse en la parte posterior del equipo. Su único requisito es el número de teléfono del servicio **PAD** de la compañía telefónica.

El Servicio de acceso remoto le permite tener acceso a la red **X.25** de dos maneras generales:

Servidor-cliente

Cliente (para los sistemas operativos **Windows™ o Windows NT**).

Ensambladores/desensambladores de paquetes (PAD) asíncronos

Metodos de Acceso

Servidor y cliente (solamente para sistemas **Windows NT**) conexiones directas.

Configuraciones X.25.

El Servicio de acceso remoto para redes **X.25** ofrece dos posibilidades de configuración para el cliente y una para el servidor:

CODESIS COMERCIALIZADORA EDITORIAL Y SISTEMAS LTDA.

Técnico en Redes y Comunicaciones para Computadores

Test No. 19

Test de Evaluación

Establecimiento del Cumplimiento de logros

Esta evaluación ha sido elaborada por el editor, CODESIS LTDA, con el objetivo de que el lector establezca el cumplimiento de logros en el proceso de aprendizaje paso a paso del Curso Técnico en Redes y Comunicaciones para Computadores.
Se trata de 20 preguntas de respuestas concretas y en ocasiones algo extensas, sobre los temas tratados en el transcurso del presente fascículo.
El lector deberá resolver por escrito las que él considere son las respuestas correctas de esta evaluación.
Para obtener el Diploma deberá enviarnos las evaluaciones, todas al final de la obra, o una por una semanalmente a nuestra dirección: Av. 22 No 40-77 Of. 302 Santafé fe Bogotá o nuestro e-mail codesis@latino.net.co

SOFTWARE

1. Explique la solución a los problemas de marcado automático.
2. Enumere las tres direcciones de marcado automático.
3. Enumere los pasos a seguir para activar Multilink en un cliente RAS.
4. Enumere los pasos a seguir para activar Multilink en un servidor RAS.
5. Enumere las características de seguridad de RAS.
6. Cómo es la asignación de acceso y permisos en RAS?
7. Enumere los seis pasos que muestran lo que ocurre durante una llamada desde un cliente a un servidor RAS.
8. Para qué sirve la codificación de datos?
9. Para qué sirve "Establecido por llamador" ?
10. Explique las dos categorías en que se dividen las auditorías.

HARDWARE

1. Explique la norma FDDI-II
2. Explique en qué consisten las dos subclases en que se puede descomponer la TPDDI.
3. Qué significa la sigla FDDI?
4. Cuáles son los tipos de tráfico que soporta MAC?
5. Enumere los temporizadores que tiene cada estación para atender primero al tráfico y luego al asícrono.
6. Qué significa la sigla DAS?
7. Que significa la sigla SAS?
8. En qué consisten las soluciones CDDI, FDDI-II y LCF-FDDI?
9. Qué es el espectro de radiofrecuencias?
10. Para qué sirven las ondas de cielo (HF)?

Técnico en Redes y Comunicaciones para Computadores

Hardware 1: Fascículo 10
Windows NT: Fascículo 20
Hardware 2: Fascículo 30
Novell 5: Fascículo 40

Contenido General de la Obra:

Software

Windows NT
- Glosario Fascículo 0
- Introducción a Windows NT
- Planificación e instalación de Windows NT Server
- Conociendo el entorno de Windows NT
- Usuarios
- Sistemas de archivos y directorios
- Ejecutar aplicaciones
- Seguridad
- Uso compartido de recursos
- Trabajo de Red
- Configuración de los componentes de la red
- Impresión
- Administración de Windows NT
- Administración de
- servicios de Impresión
- Utilidades y ordenes para usuarios
- Comunicaciones
- Conectividad con
- Netware
- TCP/IP
- Servicio de Acceso Remoto (RAS)
- Rendimiento
- Mantenimiento del sistema

Novell Netware 5.0
- Glosario (Fascículo 0)
- Introducción a Netware 5.0
- Planificación e instalación de Netware 5.0
- Instalación y administración de clientes
- Planificación de servicios de Netware 5.0
- Ordenes y utilidades de la consola
- Herramientas de administración Netware
- Administración de usuarios y objetos
- Creación y modificación de usuarios
- Asignación de derechos sobre archivos y directorios
- Administración del árbol NDS y particiones
- Administración del sistema de archivos
- Gestión de directorio y archivos
- Comandos para directorios y archivos
- Servicios de impresión en Netware y comandos
- Conexiones
- Menús de Netware
- Protección, copia y seguridad de datos
- Sistema de facturación Netware
- Herramientas y técnicas de Administración
- Comunicaciones

Hardware

- Glosario (Fascículo 0)
- Introducción
- Tipos de redes
- Componentes de una red básica
- Adaptadores
- Guía de cableado
- Modelo OSI
- Segmentos de red
- Hubs (Conectores)
- Repetidores
- Bridges
- Routers
- Switches de Redes
- Topología de redes
- Proyecto completo cableado estructurado
- Voz - datos - cableado horizontal - Cableado vertical
- Backbone

Comunicaciones

- Correo electrónico
- Modos de transmisión asincrónico, sincrónico
- Transmisión inalámbrica
- Sistema telefónico
- Satélites de
- comunicación
- Redes satelitales
- Intranet

DISTRIBUCION:

MEXICO:	DISTRIBUIDORA INTERMEX S.A. Teléfono: 230 95 00 (México D.F)
CHILE:	DISTRIBUIDORA ALFA Teléfono: 525 5599 (Santiago)
ARGENTINA:	DISTRIBUIDORA BERTRAN Teléfono: 4303 1870 (Buenos Aires)